

REMARKS

Applicants have carefully studied the outstanding Official Action mailed on 3 December 2003. This response is intended to be fully responsive to all points of rejection raised by the Examiner and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application are respectfully requested.

The Examiner notes that claims 1 - 51 have been cancelled with prejudice. Applicants respectfully point out that in the previously filed preliminary amendment claims 1 - 51 were cancelled without prejudice.

Applicants further note that the Examiner, in filling out the Office Action Summary for the present Office Action, did not acknowledge a claim of foreign priority under 35 USC §119 for the present application. Applicants respectfully point out that the present application is a Continuation Application of PCT application number PCT/IL99/00007, which application claims priority from IL 123028, filed 22 January 1998. Applicants respectfully request that the Examiner take notice of the foreign priority date.

Claims 52-63, 66, 68-75, 78-81, and 83-84 stand rejected under 35 USC §103(a) as being unpatentable over Moos (US Patent 5,881,152) and further in view of Anon, IBM TDB volume 28, number 7, pages 2861 - 2862, 1 December 1985.

Claims 64-65, 76-77, 85-86 and 88 stand rejected under 35 USC §103(a) as being unpatentable over Moos/Anon and further in view of Litman (US Patent 5988500).

Claims 67 and 82 stand rejected under 35 USC §103(a) as being unpatentable over Moos/Anon/Litman and further in view of Menzes et al., Handbook of Applied Cryptography.

Claim 87 stands rejected under 35 USC §103(a) as being unpatentable over Moos/Anon and further in view of Clark et al., A Survey of Authentication Protocol Literature 17 November 1997.

Applicants respectfully traverse the above rejections, as is now explained.

In the rejection of claim 52, Examiner asserts that "Anon teaches combining a storage medium layer, with a layer of integrated electronic circuits using a semiconductor

substrate and standard semiconductor fabrication techniques, such that the integrated circuit has memory, logic function, input/output and is able to carry out computations and thus functions as a processor (that is an embedded "chip"). The electronics on the rotating disk are coupled to external circuitry which allows them to exact power, and function as a data input/out port using wireless means, which according to the Anon could include transformer coupling, or capacitive or electro-optical. The diagram (page 2) illustrates wireless connection through two coils on[e] fixed and one attached to the rotating disk. These coils serve as the antennas, one connected to the embedded "chip" the other connected to external circuitry indicated by Anon to be a computer (hence another chip or processor)."

It is respectfully pointed out that Anon has different structure than the claimed invention. In the claimed invention, as recited in claim 52, the "first antenna [is] disposed in said DVD". In contrast, in Anon, the antenna is not at all disposed in the disk, rather as described in the text and seen clearly in Fig. 2, the first antenna is the rotating transformer 26 which is disposed on the rotor 24. "The disks 10, 12 are clamped to the rotor 24". Anon clearly distinguishes between the rotor 24 and the disk 10. Thus, in Anon, the antenna is not at all disposed in the disk, but rather is on a rotor to which the disks are clamped.

Furthermore, Moos describes a process and device for combining non-intelligent generic information storage devices and linking their information. The process compresses the stored data from a generic storage device and counts a signature count of the stored data. Moos states (col. 2 lines 61 - 67) that "a standard algorithm generates a unique compressed form of the data, as shown in step 102 of FIG. 3. This compressed data is provided with an ID (step 104) and a signature count from the chip. The data is encrypted with the secret part of the asymmetric key (step 106), and is stored in the memory area of the chip (step 108). The signature counter status is entered into the data storage medium to be protected." Persons skilled in the art will appreciate that Moos describes signing a digest of the data and does not describe encrypting the data as such. Therefore, Moos is a system and device preventing unauthorized use of content.

The claimed invention, by contrast, encrypts content (as opposed to signing

a digest of the content) thereby preventing unauthorized copying of the content. In addition, in the present invention, as opposed to Moos, the encrypted content is comprised on the media recording disk (DVD), and not in the security element. The applicants also respectfully point out that the present invention, as opposed to Moos, is optimally designed for use as part of a consumer device because of the player security chip. Moos lacks any suggestion of a player security chip.

Furthermore, the claimed invention comprises a disk chip comprising a disk security key as recited, for example, in claims 81 - 85. Moos, by contrast, describes a chip signed digest of the data.

In order to make the distinction of the claimed invention over Moos particularly clear, new dependent claims 89 - 95 have been added.

New dependent claims 89 - 91 are supported, intra-alia, by lines 16 - 19 of page 14 of the disclosure.

New dependent claim 92 is supported, intra-alia, by lines 29 - 31 of page 14 of the disclosure.

New dependent claim 93 is supported, intra-alia, by lines 5 - 7 of page 15 of the disclosure.

New dependent claim 94 is supported, intra-alia, by line 23 of page 15 of the disclosure.

New dependent claim 95 is supported, intra-alia, by lines 27 - 29 of page 15 of the disclosure.

Accordingly, it is respectfully submitted that the rejections of independent claims 52, 68 and 88, are overcome. Since claims 53-67 ultimately depend from claim 52 and claims 69-75 ultimately depend from claim 68, their rejection is also overcome.

In addition, Applicants respectfully wish to traverse points made by the Examiner regarding other claims, even though their rejection has already been overcome as stated before.

The Examiner asserts, regarding Anon, "the "chip" in this case is the

semiconductor lay[er] of the disk, is ideally suited for both static and dynamic balancing as the mass of the "chip" is spread throughout the disk."

Applicants respectfully disagree. The chip is not the semiconductor layer. Rather Anon clearly states that "on the other surface integrated electronic circuits are formed using semiconductor fabrication techniques". "Semiconductor fabrication techniques" refer to etching integrated circuits on a silicon substrate using photolithography and etching processes. This in no way means that the chip is homogeneously distributed over the entire semiconductor layer. Quite the opposite is true; it is extremely difficult if not impossible to symmetrically lay out semiconductor circuits so that the mass of the circuits is evenly distributed over the entire disk. Moreover, the circuitry is connected by hard wires 31 to rotor 24 - there is no evidence whatsoever in Anon that this is done symmetrically. Thus, it is respectfully pointed out that the mass of the "chip" is not spread throughout the disk and there is nothing inherent in Anon at all about static and dynamic balancing. Thus, the rejections to claims 55 and 56 are further traversed for these reasons.

The Examiner asserts, regarding Anon, that "such a disk is very tamper resistance (*sic*) and hard to reverse engineer, thus increasing the security over the system proposed by Moos."

Applicants respectfully disagree. Anon merely forms integrated electronic circuits on the outer surface of the disk using semiconductor fabrication techniques. There is no attempt to make the circuits tamper proof, and no motive or attempt is discussed at all. On the contrary, as described and shown in the diagram (page 2) of Anon, it would be straightforward for a "hacker" to reverse engineer the electronics, because the electronics are right on the upper surface and exposed for all to see. Since the electronics are totally exposed, it is not understood at all why the Examiner calls this "very tamper resistant" - any sharp or blunt instrument could easily damage it and tamper with it. Thus, the rejections to claims 59 and 60 are further traversed for these reasons.

The Examiner asserts, regarding Anon, that "the limitation to make the chip in the player detachable (separable) would also be obvious to one of ordinary skill in the art

at the time that the invention were made because it would allow upgrades."

The basic considerations that apply to obviousness rejections under MPEP §2141 are as follows:

- a) the claimed invention must be considered as a whole;
- b) the references must be considered as a whole and must suggest the desirability and thus the obviousness of making the combination;
- c) the references must be viewed without the benefit of impermissible hindsight vision afforded by the claimed invention; and
- d) reasonable expectation of success is the standard by which obviousness is determined.

When the prior art itself fails to meet even one of the above criteria the cited art does not satisfy 35 USC §103(a) and prevents the establishment of the required *prima facie* case of obviousness by the Examiner. See In re Oetiker, 977 F.2d 1443, 1445 (Fed. Cir. 1992); see also In re Rijckaert, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993). Moreover, to establish the required case of *prima facie* obviousness, the Examiner is required to demonstrate that the prior art discloses or suggests all the critical elements of the invention, without reference to applicants' specification, and that the existence of these elements enables one skilled in the art to practice the invention. See In re Vaeck, 947 F.2d 488 (Fed. Cir. 1991).

It is respectfully submitted that the prior art cited by the Examiner does not suggest or disclose a "player security chip being detachable from said DVD player". Moreover, if the prior art methodology must be modified in any way to practice the instant invention the prior art citation must *also* render obvious these modifications or provide a reasonable expectation for the successful practice of the invention with the necessary modifications. Therefore, it is respectfully submitted that the rejection of claims 52 (detachable) and 61 (upgradable) are not proper because the prior art fails to teach these features and fails to render them obvious.

Furthermore, the Examiner rejected claim 52 on the basis that "the limitation to make the chip in the player detachable (separable) would also be obvious to one of ordinary skill in the art at the time the invention were made (*sic*) because it would allow upgrades." The prior art of record does not show or suggest the indicated feature. The Examiner is respectfully asked to provide such a reference and to supply a motivation to make the player chip detachable. Absent such a reference and a motivation to make the player chip detachable, rejection is improper.

Likewise, the Examiner rejected claim 58 on the basis that "if it is not already inherent that the decoder is in the read/right (*sic*) unit of the disk storage reader (player), then one of ordinary skill of the art at the time of the invention would have strong motivation to place it there because the read/write functions are tied up with encoding and decoding." The prior art of record does not show or suggest the indicated feature. The Examiner is respectfully asked to provide such a reference and to supply a motivation to place the decoder in the read/write unit of the disk storage reader (player). Absent such a reference and a motivation to place the decoder in the read/write unit of the disk storage reader (player), rejection is improper.

Additionally, the Examiner rejected claims 59 - 60 on the basis that "one of ordinary skill in the art at the time the invention was make (*sic*) would have been motivated to apply the standard methods of tampering heeding the warning of Moos to implement tamper protection to the security chip in the player." The prior art of record does not show or suggest the indicated feature. The Examiner is respectfully asked to provide such a reference and to supply a motivation to "apply the standard methods of tampering heeding the warning of Moos to implement tamper protection to the security chip in the player." Absent such a reference and a motivation to "apply the standard methods of tampering heeding the warning of Moos to implement tamper protection to the security chip in the player," rejection is improper.

The Examiner asserts, regarding claim 78, that "Moos/Anon is silent with regards to who should known (*sic*) the keys, however, one of ordinary skill in the art would

have no motivation to give the key to the disk vendor because they are not involved in the encryption of the disk content."

Applicants respectfully wish to point out that this assertion is contradicted by the disclosure of Moos, col. 2, lines 61-67: "A standard algorithm generates a unique compressed form of the data, as shown in step 102 of FIG. 3. This compressed data is provided with an ID (step 104) and a signature count from the chip. The data is encrypted with the secret part of the asymmetric key (step 106), and is stored in the memory area of the chip (step 108). The signature counter status is entered into the data storage medium to be protected."

It is clear that Moos uses the data stored in the disk as part of the encryption in the chip. Thus in Moos the disk vendor is indeed involved in the encryption of the disk content. Thus, the rejection to claim 78 is respectfully traversed. Since claims 80-86 ultimately depend from claim 78, their rejection is also overcome.

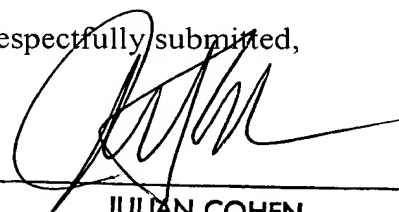
Regarding the Examiner's rejection of claim 84, the Examiner remarks, concerning Moos, that "it is inherent in this system that the public key must be kept secret and this is the reason why it is stored on the disk chip." Moos in fact states (col. 2, lines 29 - 33), "the intelligent data storage medium (chip) 10 contains an asymmetric key comprising a public and a secret part, a symmetric key for authentication, an ID and a signature counter 14. Due to its design, it is capable of actively safeguarding these components." The applicant respectfully point out that Moos himself distinguishes between the public and secret parts of the asymmetric key. The public key in Moos is not kept secret. Thus, Moos teaches away from the present invention as claimed in claim 84.

Although Applicants respectfully traverse the rejections of claims 79 and 87, nevertheless for the purposes of expedited allowance, these claims have been canceled.

Accordingly, it is respectfully submitted that claims 52-78, 80-86, 88 and 89 - 95 are in a condition for allowance.

In view of the foregoing remarks, it is respectfully submitted that the present application is now in condition for allowance. Favorable reconsideration and allowance of the present application are respectfully requested.

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Julian Cohen', is written over a horizontal line.

JULIAN COHEN
c/o LADAS & PARRY
26 WEST 61st STREET
NEW YORK, N. Y. 10023
Reg. No. 20302 (212) 708-1887